**INFORMATION SECURITY POLICY**

**Purpose**

The purpose of this Policy is to safeguard information within a secure environment belonging to Synergy Pay Solutions. (the Group) and its stakeholders (third parties, customers or customers and the general public).
This policy informs the Group's staff, all roles, all divisions within the Company, and all controlled legal entities entitled to use Group facilities, of the principles governing information holding, use and disposal.
It is the goal of the Group that:

- Information will be protected against unauthorized access or misuse.
- Confidentiality of information will be secured.
- Integrity of information will be maintained.
- Availability of information / information systems is maintained for service delivery.
- Business continuity planning processes will be maintained.
- Regulatory, contractual and legal requirements will be complied with.
- Physical, logical, environmental and communications security will be maintained.
- Infringement of this Policy may result in regulatory sanctions or criminal prosecution.
- When information is no longer of use, it is disposed of in a suitable manner.
- All information security incidents will be reported to the Director of Information and Communication Technology (ICT) Systems, and investigated through the appropriate management channel.

Information relates to:

- Electronic information systems (software, computers, and peripherals) owned by the Group whether deployed or accessed on or off site.
- The Group's computer network used either directly or indirectly.
- Hardware, software and data owned by the Group.

**The Policy**

The Group requires all users to exercise a duty of care in relation to the operation and use of its information systems.

a. <u>Authorized users of information systems</u>

All users of Group information systems must be formally authorized by appointment as a staff member, with the exception of information published for public consumption. Authorized users will have a unique identity for the user. It is not appropriate to reveal any password associated with a user identity to any other person.

Authorized users will pay due care and attention to protect Group information in their personal possession. Confidential, personal or private information must not be copied or transported without consideration of:

- Permission of the information owner
- The risks associated with loss or falling into the wrong hands
- How the information will be secured during transport and at its destination.

b. Information System Owners

Head/Directors who are responsible for information systems are required to ensure that:

1. Systems are adequately protected from unauthorized access.
2. Systems are secured against theft and damage to a level that is cost-effective.
3. Adequate steps are taken to ensure the availability of the information system, commensurate with its importance (Business Continuity).
4. Electronic data can be recovered in the event of loss of the primary source. I.e. failure or loss of a computer system. It is incumbent on all system owners to backup data and to be able to restore data to a level commensurate with its importance (Disaster Recovery).
5. Data is maintained with a high degree of accuracy.
6. Systems are used for their intended purpose and that procedures are in place to rectify discovered or notified misuse.
7. Any electronic access logs are only retained for a justifiable period to ensure compliance with the data protection, investigatory powers and freedom of information acts.
8. Any third parties entrusted with Group data understand their responsibilities with respect to maintaining its security.

c.Personal Information

No privacy rights are granted to authorized users of information systems in relation to their use of Group information systems. Group officers who are properly licensed can access or track personal data contained in any group information system (mailboxes, web access logs, file stores, etc.).

d. Individuals in breach of this policy are subject to regulatory actions (staff) at the instigation of the Director with responsibility for the relevant information system, including referral to the Police where appropriate.
The Group will take legal action to ensure that its information systems are not used by unauthorized persons.

**Ownership**

a. The Director of ICT Systems has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.

Information system owners are responsible for the implementation of this Policy within their area, and to ensure adherence.